Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Калістого Дмитра Сергійовича*

академічної групи *125-18зск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка засобів захисту інформаційно-комунікаційної системи підприємства «Фотон» від зловмисної масової розсилки повідомлень*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Калістому Дмитру Сергійовичу*** **академічної групи** ***125-18зск-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка засобів захисту інформаційно-комунікаційної системи підприємства «Фотон» від зловмисної масової розсилки повідомлень***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Дослідження і розробка методології захисту корпоративних інформаційних систем від загроз пов'язаних із зловмисною масовою розсилкою повідомлень	29.03.2021
Розділ 2	Аналіз загроз інформаційної безпеки корпоративних інформаційних систем, які пов'язані із зловмисною масовою розсилкою повідомлень, проаналізувати методи протидії цим загрозам та розробити методологія захисту від даного типу загроз	24.05.2021
Розділ 3	Розрахунок собівартості впровадження системи захисту від загроз пов'язаних із зловмисною масовою розсилкою повідомлень та обґрунтування економічної доцільності її впровадження	14.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Об'єкт дослідження: система захисту корпоративних інформаційних мереж від загроз пов'язаних із зловмисною масовою розсилкою повідомлень.

Мета роботи: розробка методології захисту корпоративних інформаційних систем від загроз пов'язаних із зловмисною масовою розсилкою повідомлень.

Новизна результатів, що очікуються, полягає у розробці методики для вирішення проблем, які виникають внаслідок загроз пов'язаних із зловмисною масовою розсилкою повідомлень за допомогою програмних комплексів та організаційних заходів.

У спеціальній частині виконано аналіз загроз інформаційної безпеки корпоративних інформаційних систем, які пов'язані із зловмисною масовою розсилкою повідомлень, проаналізовані методи протидії цим загрозам та розроблена методологія захисту від даного типу загроз.

В економічному розділі проведено розрахунок капітальних та експлуатаційних витрат на проектування та впровадження нового комплексу для захисту від спаму та розраховано економічний ефект від впровадження даного комплексу.

СПАМ, МЕТОДОЛОГІЯ ЗАХИСТУ, КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ, НЕДІЛОВА КОРЕСПОНДЕНЦІЯ, ЕЛЕКТРОННА ПОШТА, ЗАХИСТ ВІД МАСОВОЇ РОЗСИЛКИ.

РЕФЕРАТ

Пояснительная записка: ___ с, ___ рис, ___ табл, ___ приложений, __ источников;

Объект исследования: система защиты корпоративных информационных сетей от угроз связанных с злонамеренной массовой рассылкой сообщений.

Цель работы: разработка методологии защиты корпоративных информационных систем от угроз связанных с злонамеренной массовой рассылкой сообщений.

Новизна результатов, ожидается, заключается в разработке методики для решения проблем, возникающих в результате угроз связанных с злонамеренной массовой рассылкой сообщений с помощью программных комплексов и организационных мероприятий.

В специальной части выполнен анализ угроз информационной безопасности корпоративных информационных систем, связанных с злонамеренной массовой рассылкой сообщений, проанализированы методы противодействия этим угрозам и разработана методология защиты от данного типа угроз.

В экономическом разделе проведен расчет капитальных и эксплуатационных затрат на проектирование и внедрение нового комплекса для защиты от спама и рассчитан экономический эффект от внедрения данного комплекса.

СПАМ, МЕТОДОЛОГИЯ ЗАЩИТЫ, КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, НЕДЕЛОВАЯ КОРРЕСПОНДЕНЦИЯ, ЭЛЕКТРОННАЯ ПОЧТА, ЗАЩИТА ОТ МАССОВОЙ РАССЫЛКИ.

ABSTRACT

Explanatory note: __ p., __ fig., __ tab., __ additions, __ sources.

Object of research: the system of protection of corporate information networks from threats related to malicious mass messaging.

Purpose: to develop a methodology for protecting corporate information systems from threats related to malicious mass messaging.

The novelty of the expected results is the development of a methodology for solving problems arising from the threats associated with malicious mass messaging through software packages and organizational measures.

In the special part the analysis of threats of information security of corporate information systems which relate to malicious mass distribution of messages is executed, the methods of counteraction to these threats are analyzed and the methodology of protection against this type of threats is developed.

In the economic section, the calculation of capital and operating costs for the design and implementation of a new complex for protection against spam and calculated the economic effect of the implementation of this complex.

SPAM, PROTECTION METHODOLOGY, CORPORATE INFORMATION SYSTEMS, NON-BUSINESS CORRESPONDENCE, E-MAIL, PROTECTION AGAINST MASS POSTING.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

Д – доступність;

ЕОМ – електрона обчислювальна машина;

К – конфіденційність;

КЗЗ – комплекс засобів захисту;

КІС – корпоративна інформаційна система;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна об’єднувальна;

НД – нормативний документ;

ТЗІ – технічний захист інформації;

ПЗ – програмне забезпечення;

Ц – цілісність.

ЗМІСТ

ВСТУП

Корпоративна інформаційна система – це інформаційна система, що підтримує оперативний та управлінський облік на підприємстві і надає інформацію для оперативного прийняття управлінських рішень. [1]

Головним завданням такої системи є інформаційна підтримка виробничих, адміністративних та управлінських процесів, які формують продукцію або послуги підприємства.

Однією із значних загроз електронної пошти і всій корпоративній системі в цілому становлять загрози пов'язані із зловмисною масовою розсилкою повідомлень.

Спам – не замовлені попередньо споживачами електронні повідомлення, які або є масовими, або в яких не наведено достовірні відомості про повну назву, власну поштову чи електронну адресу замовника чи відправника цих повідомлень, або подальше отримання яких споживач не може припинити шляхом інформування про це замовника чи відправника. [2]

Захист від спаму має дуже велике значення в корпоративних інформаційних мережах, оскільки за різними джерелами від 70 до 90% електронних повідомлень це неділова кореспонденція, що призводить до таких наслідків:

- зниження продуктивності роботи інформаційної системи;
- відчутне зниження продуктивності праці у персоналу організації, через очищення поштових скриньок від спаму;
- перехід за посиланнями на розважальні ресурси, що згодом впливає на трудову активність персоналу і доходи організації;
- значне збільшення часу пошуку потрібних листів або інформації;
- зниження працездатності або ж відмова в обслуговуванні поштової системи і поштових серверів через великого потоку даних;
- «фішинг» – вид інтернет-шахрайства, при якому зловмисник змушує користувача виконати певні дії шляхом відправки листів жертві від імені довіреного відправника;

- загромадження ресурсів інформаційної системи (заняття дискового простору під неділову пошту).

Підхід до захисту повинен бути всебічним і комплексним – необхідно поєднувати організаційні заходи з використанням відповідних технічних засобів. До організаційних заходів належать розробка і впровадження в компанії політики використання електронної пошти. Технічні засоби повинні забезпечити виконання цієї політики, як за рахунок моніторингу поштового трафіку, так і за рахунок адекватного реагування на порушення.

Спочатку необхідно сформулювати політику, скласти правила використання електронної пошти, визначити, як створена система повинна реагувати на певні порушення даної політики і після цього впроваджувати програмно-апаратний комплекс захисту від загроз пов’язаних із зловмисною масовою розсилкою повідомлень.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Корпоративні інформаційні системи

Корпоративна інформаційна система – це інформаційна система, що підтримує оперативний та управлінський облік на підприємстві і надає інформацію для оперативного прийняття управлінських рішень. [1]

Головним завданням такої системи є інформаційна підтримка виробничих, адміністративних та управлінських процесів, які формують продукцію або послуги підприємства.

Основне призначення корпоративних систем - своєчасне надання несуперечливої, достовірної та структурованої інформації для прийняття управлінських рішень.

КІС створюються з урахуванням того, що вони повинні здійснювати узгоджене керування даними в межах підприємства (організації), координувати роботу окремих підрозділів, автоматизувати операції з обміну інформацією, як в межах окремих груп користувачів, так і між територіально віддаленими підрозділами. Основою для побудови таких систем служать локальні обчислювальні мережі.

КІС мають наступні характерні риси:

- охоплення великого числа завдань управління підприємством;
- детальна розробка узагальненої моделі документообігу підприємства;
- наявність вбудованих інструментальних засобів, що дозволяють користувачеві самостійно розвивати можливості системи і адаптувати її під себе;
- розвинена технологія об’єднання і консолідація даних віддалених підрозділів.

1.1.1 Роль електронної пошти в КІС

Електронна пошта - один з найбільш широко використовуваних видів сервісу, як у корпоративних мережах, так і в Інтернет. Вона є не просто способом доставки повідомлень, а найважливішим засобом комунікації, розподілу інформації і управління різними процесами в бізнесі. Роль електронної пошти стає очевидною, якщо розглянути функції, які виконує пошта:

- забезпечує внутрішній і зовнішній інформаційний обмін;
- з компонентом системи документообігу;
- формує транспортний протокол корпоративних додатків;

Завдяки виконанню цих функцій електронна пошта вирішує одне з найважливіших на даний момент завдань – формує єдиний інформаційний простір. У першу чергу це стосується створення спільної комунікаційної інфраструктури, яка спрощує обмін інформацією між окремими людьми, підрозділами однієї компанії і різними організаціями.

Використання електронної пошти для обміну інформацією між людьми як всередині окремо взятої організації, так і за її межами здатне корінним чином змінити технології і методи ведення справ. Перехід до обміну документами в електронному вигляді відкриває нові можливості для підвищення ефективності праці та економії коштів і часу.

Електронна пошта має ряд переваг у порівнянні зі звичайними способами передачі повідомлень (традиційна пошта або факсимільний зв'язок). До них належать такі:

- оперативність і легкість використання;

Електронна пошта – це глобальна система, що дозволяє передавати листи в будь-яку точку світу за лічені хвилини, незалежно від часу доби. Відправка і прийом повідомлень електронної пошти не вимагають глибоких знань комп'ютерних технологій, завдяки чому цей сервіс широко застосовується не тільки в бізнесі, але і для особистого спілкування. Крім того сучасні умови вимагають оперативного реагування на процеси, що відбуваються в бізнесі.

Електронна пошта дозволяє збирати інформацію, приймати рішення і доводити їх до різних підрозділів компанії та партнерів по бізнесу. [2]

- доступність практично в будь-якому місці;

Головна перевага електронної пошти – її доступність. І хоча величезні простори ще не до кінця освоєні електронікою, стрімкий розвиток електронних комунікацій, в кінцевому рахунку, призведе до того, що "глобальна павутина" покриє всю земну кулю.

- універсальність форматів листів і вкладень;

Зручність використання електронної пошти полягає в тому, що вона здатна "переносити" великі обсяги інформації різних форматів даних. В одному листі можуть бути одночасно передані графічна, відео, текстова інформація, файли баз даних, додатків і т.п.

- низька собівартість;

Відправити електронного листа коштує значно дешевше, ніж звичайне або зробити міжміський або тим більше міжнародний телефонний дзвінок. Електронна пошта дозволяє розсилати листи відразу декільком адресатам без додаткових витрат.

- надійність і швидкість інфраструктури доставки;

Так як електронна пошта пересилається безпосередньо з сервера відправника на сервер одержувача по каналах Інтернет, цей процес протікає швидко, навіть якщо ці сервери розташовані на протилежних сторонах земної кулі. Фактично на передачу текстового повідомлення, наприклад, з Росії в Америку потрібно не більше 1-2 хвилин.

- використання для обробки електронної пошти спеціального програмного забезпечення.

Електронний характер листа дозволяє проводити його обробку за допомогою додаткового програмного забезпечення. При цьому види обробки електронної пошти залежать від характеру діяльності організації. Це може бути: створення бази даних електронної пошти, формування різних звітів, проведення

аналізу діяльності компанії і т.п. Все це дозволяє створити єдину систему управління документообігом, повністю інтегровану з іншими інформаційними процесами в компанії.

1.1.2 Загрози безпеки електронної пошти

Електронна пошта володіє численними перевагами, але саме через ці переваги виникають основні загрози, пов'язані з її використанням. Наприклад, доступність електронної пошти перетворюється на недолік, коли користувачі починають застосовувати пошту для розсилки спаму, легкість у використанні і безконтрольність призводить до витоку інформації, можливість пересилання різних форматів документів – до поширення вірусів і т.д. [6]

В кінцевому підсумку будь-яка з цих загроз може призвести до серйозних наслідків для компанії. Це і втрата ефективності роботи, і зниження якості послуг інформаційних систем, і розголошення конфіденційної інформації. Недостатня увага до даної проблеми загрожує значними втратами в бізнесі, а в деяких випадках навіть залученням до юридичної відповідальності у зв'язку з порушенням законодавства.

Компанія піддається впливу даним загрозам в силу ряду властивостей електронної пошти. Наприклад, завдяки застосуванню MIME-стандарту електронна пошта може переносити великі об'єми інформації різних форматів даних у вигляді прикріплених до повідомлень файлів. Такою можливістю відразу скористалися зловмисники. Така перевага електронної пошти перетворилася на загрозу, оскільки електронна пошта стала являти собою практично ідеальне середовище для перенесення різного роду небезпечних вкладень, а саме комп'ютерних вірусів, шкідливих програм, фітингу і т.д. Якщо належний контроль за використанням електронної пошти не забезпечений, це може призвести до надзвичайно серйозних наслідків і навіть завдати непоправної шкоди. Позбутися від даного ризику можна лише шляхом блокування листів з "небезпечними" вкладеннями, а також антивірусної

перевірки прикріплених файлів. На практиці ж оптимальним засобом може виявитися блокування певних типів файлів.

Ще однією загрозою електронній пошті являється її резервне копіювання повідомлень, яке може залишатися на персональних комп'ютерах відправника і одержувача або в мережі компаній, де вони працюють. Якщо електронне поштове повідомлення надіслано через комерційну службу або через Інтернет, то воно буде передаватися через кілька різних серверів. Кожен сервер в ланцюжку між відправником та одержувачем може зберегти копію повідомлення в своїх архівах. Навіть методичне з'ясування місцезнаходження кожної копії електронного листа з наступним його видаленням не дає ніякої гарантії того, що повідомлення не залишилося на жорсткому диску комп'ютера або сервера. За допомогою широко доступного програмного забезпечення навіть рядовий користувач зможе відновити повідомлення електронної пошти після того, як його нібито видалили.

Всі ці особливості, а також простота копіювання електронного повідомлення і неможливість контролю даної операції призводять до того, що співробітник може передати корпоративну інформацію будь-якій кількості людей як всередині, так і за межами компанії анонімно і без відповідного дозволу, відразу або після закінчення будь-якого часу. При цьому, така інформація може представляти собою службову інформацію компанії (тексти договорів, відомості про плановані угоди тощо), паролі, системні дані, вихідні коди програм або іншу конфіденційну інформацію. Це загрожує серйозними порушенням конфіденційності і може призвести до неприємних наслідків для компанії.

На відміну від паперової кореспонденції, електронну пошту дуже легко ненавмисно відправити за невірною адресою. Причиною цього може бути як невміле використання адресних книг, так і помилка в адресі одержувача або, що ще гірше, випадковий вибір опції, що передбачає розсилку повідомлення великій групі користувачів, у той час як повідомлення є конфіденційним.

Щоб забезпечити захист від витоку конфіденційної інформації з мережі, необхідно здійснювати контроль адресатів, фільтрацію переданих даних на наявність в текстах повідомлень або в прикріплених до електронного листа файлах слів і виразів, що мають відношення до "закритої" тематики, здійснювати розмежування доступу різних категорій користувачів до архівів електронної пошти та т.п.

Також однією зі значних загроз електронної пошти і всій корпоративній системі в цілому становлять загрози пов'язані із зловмисною масовою розсилкою повідомлень.

Спам – не замовлені попередньо споживачами електронні повідомлення, які або є масовими, або в яких не наведено достовірні відомості про повну назву, власну поштову чи електронну адресу замовника чи відправника цих повідомлень, або подальше отримання яких споживач не може припинити шляхом інформування про це замовника чи відправника. [2]

Захист від спаму має дуже велике значення в корпоративних інформаційних мережах, оскільки за різними джерелами від 70 до 90% електронних повідомлень це неділова кореспонденція, що призводить до таких наслідків:

- зниження продуктивності роботи інформаційної системи;
- відчутне зниження продуктивності праці у персоналу організації, через очищення поштових скриньок від спаму;
- перехід за посиланнями на розважальні ресурси, що згодом впливає на трудову активність персоналу і доходи організації;
- значне збільшення часу пошуку потрібних листів або інформації;
- зниження працездатності або ж відмова в обслуговуванні поштової системи і поштових серверів через великого потоку даних;
- "фішинг" – вид інтернет-шахрайства, при якому зловмисник змушує користувача виконати певні дії шляхом відправки листів жертві від імені довіреного відправника;

- загромадження ресурсів інформаційної системи (заняття дискового простору під неділову пошту).

Як правило, це листи, що містять нав'язливі пропозиції найрізноманітніших послуг, товарів і т.п. Велика кількість не ділової кореспонденції завантажує канали, "засмічує" поштові ящики, забирає час на видалення непотрібних листів і підвищує ймовірність випадкового видалення потрібних. Звичайно розсилка, наприклад, повідомлень рекламного характеру, прямо не переслідує мети "засмітити" поштову мережу організації, проте побічно призводить до негативних наслідків. Використання списків розсилки, в яку можуть входити всі користувачі однієї корпоративної мережі, та отримання одночасно всіма цими користувачами повідомлень рекламного характеру загрожує компанії зниженням продуктивності її мережевих ресурсів.

1.3 Нормативно правова база

Першою державою, яка вдалася до законодавчих обмежень, що стосуються розповсюдження спаму, є США. Починаючи з 1998 р., в різних штатах стали з'являтися спеціальні закони про спам. Вони передбачають обов'язковість ідентифікації відправника та наявності механізму відписки (тобто відмови від подальшого отримання подібних повідомлень), а також заборона фальсифікації заголовків листів. В основному закони спрямовані проти комерційного спаму, але в ряді штатів заборонено і некомерційний спам (Коннектикут, Іллінойс, Луїзіана, Вірджинія). За порушення даних законодавчих обмежень встановлена кримінальна відповідальність (штраф до $ 10 000 або позбавлення волі на строк до 5 років) і цивільно-правова відповідальність (відшкодування одержувачу по $ 500 за кожне повідомлення і провайдеру до $ 25 000 за день розсилки).

Пізніше цей досвід США був перейнятий європейськими країнами. У Норвегії заборонений прямий маркетинг з використанням електронної пошти без попередньої згоди на нього одержувача інформації.

У Фінляндії з 1999 р. діє закон, згідно з яким дозволяється розсилати інформацію тільки попередньо підписалися на неї фізичним особам.

В Австрії внесені поправки в «Закон про телекомунікації», які дозволяють у випадку розсилки спаму вимагати від його відправника суму відшкодування шкоди в розмірі до 500 000 австрійських шилінгів, а в Італії за ті самі дії встановлена сума відшкодування від 500 до 5000 євро.

В Україні також був прийнятий міжнародний досвід правового регулювання даного явища. В українському законодавстві термін «спам» отримав своє визначення в 2005 році в Правилах надання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 09.08.2005 № 720. Згідно з цим визначенням, терміном «спам» позначаються електронні повідомлення, попередньо не замовлені споживачами, які або є масовими, або в яких не наведено достовірні відомості про повну назву, власну поштову або електронну адресу замовника або відправника цих повідомлень, або подальше отримання яких споживач не може припинити шляхом інформування про це замовника або відправника.

Таким чином, основною ознакою спаму, є те, що повідомлення попередньо не замовлено споживачем (одержувачем). При цьому, однієї цієї ознаки не достатньо для того що б повідомлення було кваліфіковано як спам. Для цього необхідно також наявність хоча б однієї з таких ознак:

- повідомлення є масовими;
- в повідомлення відсутні достовірні відомості про повну назву, власну поштову, або електронну адресу замовника, або відправника повідомлення;
- подальше отримання повідомлення не може бути припинено одержувачем шляхом інформування про це замовника або відправника.

Пунктом 434 Правил надання та отримання телекомунікаційних послуг встановлено, що споживач (абонент) не може, зокрема, замовляти і пропонувати розсилку спаму, розсилати спам.

Порушення Правил надання та отримання телекомунікаційних послуг, згідно пункту 16 цих же Правил, є підставою для скорочення або припинення надання споживачеві (абоненту) телекомунікаційних послуг.

Однак законодавство України містить і більш суворі санкції за розсилку спаму. Зокрема, статтею 363-1 Кримінального кодексу України передбачена кримінальна відповідальність за умисне масове розповсюдження повідомлень електронного зв'язку, що здійснюється без отримання попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у вигляді штрафу від 8500 до 17000 гривень або обмеження свободи до трьох років.

Якщо ж ці дії були вчинені повторно або змовою групи осіб і привели до заподіяння значної шкоди, то до осіб, які вчинили такі дії можуть бути застосовані санкції у вигляді обмеження або позбавлення волі на строк до 5 років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років з конфіскацією програмних або технічних засобів.

Створення системи захисту від загроз пов'язаних із зловмисною масовою розсилкою повідомлень регулюються наступними документами:

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах";
- НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі";
- Закон України "Про електронні документи та електронний документообіг";
- постанова Кабінету міністрів України "Про затвердження Правил надання та отримання телекомунікаційних послуг".

1.4 Захист корпоративної електронної пошти від загроз пов'язаних із зловмисною масовою розсилкою повідомлень.

1.4.1 Методи захисту від спаму

Підхід до захисту повинен бути всебічним і комплексним – необхідно поєднувати організаційні заходи з використанням відповідних технічних засобів. До організаційних заходів належать розробка і впровадження в компанії політики використання електронної пошти. Технічні засоби повинні забезпечити виконання цієї політики, як за рахунок моніторингу поштового трафіку, так і за рахунок адекватного реагування на порушення. [8]

Спочатку необхідно сформулювати політику, скласти правила використання електронної пошти, визначити, як створена система повинна реагувати на певні порушення даної політики і тільки потім переводити правила на комп'ютерну мову того засобу, який використовується для контролю виконання положень політики використання електронної пошти.

До таких технічних засобів відноситься спеціальне програмне забезпечення, так звана система контролю вмісту електронної пошти. У функції таких систем входить контроль поштового трафіку і ведення архіву листування по електронній пошті. До даних систем пред'являються наступні вимоги:

а) проведення текстового аналізу;

б) фільтрація переданих даних:

- за розміром і обсягом даних;
- за кількістю вкладень в електронні листи;
- по типу файлів (вкладених в електронну пошту);
- за адресою електронної пошти.

в) контроль використання поштових ресурсів та розмежування доступу до них різних категорій користувачів;

г) відкладену доставку повідомлень електронної пошти за розкладом;

д) ведення повнофункціонального архіву електронної пошти;

Виконання цих вимог забезпечується застосуванням в засобах захисту певних механізмів. До таких механізмів можуть належати:

- рекурсивна декомпозиція (спеціальний алгоритм, який застосовується для розбору повідомлень електронної пошти на складові компоненти з подальшим аналізом їх вмісту);
- визначення типу файлів за сигнатурі;
- повнотекстовий пошук по архіву електронної пошти і т.п.

1.4.2 Аналіз програмно-апаратні комплексів захисту від спаму

Комплекси захисту від спаму – це програмне і апаратне забезпечення, здатне аналізувати зміст листа по різних компонентам і структурі, а також адреси відправників, для аналізу повідомлення на ознаки спаму.

До особливостей даних продуктів відносяться:

- застосування при аналізі змісту спеціально розробленої політики використання електронних листів;
- здатність здійснювати "рекурсивну декомпозицію" електронних листів;
- можливість розпізнавання реальних форматів файлів незалежно від різних способів їх маскування (спотворення розширення файлів, архівування файлів і т.п.);
- аналіз безлічі параметрів повідомлення електронної пошти;
- аналіз вмісту повідомлення електронної пошти і прикріплених файлів на наявність заборонених до використання слів і виразів.

1.4.2.1 Вимоги до програмно-апаратних комплексів захисту від спаму

Спектр можливостей всіх категорій систем контролю вмісту електронної пошти досить широкий і істотно змінюється в залежності від виробника. Проте до всіх систем пред’являються найбільш загальні вимоги, які дозволяють вирішувати завдання, пов’язані з контролем поштового трафіку.

Найпершими вимогами до таких систем мають бути повнота і адекватність.

Повнота – це здатність систем контролю забезпечити найбільш глибоку перевірку повідомлень електронної пошти. Це передбачає, що фільтрація повинна проводитися по всіх компонентах повідомлення. Умови перевірки листів повинні враховувати всі проблеми, ризики і загрози, які можуть існувати в організації, що використовує систему електронної пошти.

Адекватність – це здатність систем контролю вмісту якомога повніше втілювати словесно сформульовану політику використання електронної пошти, мати всі необхідні засоби реалізації написаних людьми правил в зрозумілі системі умови фільтрації.

До інших загальних вимог відносяться:

- текстовий аналіз електронної пошти (Аналіз ключових слів і виразів за допомогою вбудованих словників). Дана можливість дозволяє виявити і своєчасно запобігти витоку конфіденційної інформації, встановити наявність непристойного або забороненого змісту, зупинити розсилку спаму, а також передачу інших матеріалів, заборонених політикою безпеки. При цьому якісний аналіз тексту повинен припускати морфологічний аналіз слів, тобто система повинна мати можливість генерувати і визначати всілякі граматичні конструкції слова. Ця функція набуває великого значення у зв'язку з особливостями російської мови, в якому слова мають складні граматичні конструкції;
- контроль відправників та одержувачів повідомлень електронної пошти. Дана можливість дозволяє фільтрувати поштовий трафік, тим самим реалізуючи деякі функції міжмережевого екрану в поштовій системі;
- розбір електронних листів на компоненти (MIME-заголовки, тіло листа, прикріплені файли і т.п.). Усунення небезпечних вкладень і подальший збір компонентів листа воєдино, причому з можливістю додавати до повідомлення електронної пошти необхідні для адміністраторів безпеки елементи (наприклад, попередження про наявність вірусів або "забороненого" тексту в зміст листа);

- блокування або затримка повідомлень великого розміру до того моменту, коли канал зв'язку буде найменше завантажений (наприклад, в неробочий час).Циркуляція в поштовій мережі компанії таких повідомлень може привести до перевантаження мережі, а блокування або відкладена доставка дозволить цього уникнути;

- розпізнавання графічних, відео і звукових файлів. Як правило, такі файли мають великий розмір, і їх циркуляція може привести до втрати продуктивності мережевих ресурсів. Тому здатність розпізнавати і затримувати дані типи файлів дозволяє запобігти зниженню ефективності роботи компанії;

- обробка архівних файлів. Це дає можливість перевіряти стислі файли на вміст у них різних небезпечних вкладень;

- розпізнавання виконуваних файлів. Як правило, такі файли мають великий розмір і рідко мають відношення до комерційної діяльності компанії. Крім того, виконувані файли є основним джерелом зараження вірусами, що передаються з електронною поштою. Тому здатність розпізнавати і затримувати дані типи файлів дозволяє запобігти зниженню ефективності роботи компанії і уникнути зараження системи;

- здатність визначати число вкладень в повідомленнях електронної пошти. Пересилання електронного листа з великою кількістю вкладень може призвести до перевантаження мережі, тому контроль за дотриманням визначених політикою інформаційної безпеки обмежень на кількість вкладень забезпечує збереження ресурсів корпоративної мережі;

- контроль і блокування програм-закладок (Cookies), шкідливого мобільного коду (Java, ActiveX, JavaScript, VBScript і т.д.), а також файлів, що здійснюють автоматичну розсилку (так звані "Automatic Mail-to"). Ці види вкладень є вкрай небезпечними і призводять до витоку інформації з корпоративної мережі;

- категоризація ресурсів поштової системи компанії ("адміністративний", "відділ кадрів", "фінанси" і т.д.) і розмежування доступу

співробітників компанії до різних категорій ресурсів мережі (в т.ч. і в залежності від часу доби);

- реалізація різних варіантів реагування, в тому числі: видалення або тимчасове блокування повідомлення; затримка повідомлення та переміщення його в карантин для подальшого аналізу; "лікування" зараженого вірусом файлу; повідомлення адміністратора безпеки або будь-якого іншого адресата про порушення політики безпеки і т.п.;

- можливість модифікації даних, яка передбачає, наприклад, видалення неприйнятних вкладень і заміну їх на тексти заданого змісту. Така можливість дозволить адміністратору видаляти з листів прикріплені файли, тип яких заборонений політикою безпеки компанії. До таких типів можуть відноситися відео та звукові файли, які не мають відношення до діяльності компанії. А це, в кінцевому підсумку, дозволить уникнути зараження мережі вірусами і домогтися від співробітників продуктивного використання поштового сервісу;

- ведення повнофункціонального архіву електронної пошти, здатного забезпечити зберігання в інтернет режимі великої кількості електронної пошти з високим рівнем доступності даних. На підставі збереження даних в архіві інформації, можливо проводити подальший аналіз поштового потоку компанії, коригувати роботу системи, здійснювати аналіз інцидентів, пов'язаний зі зловживанням співробітниками компанії поштовим сервісом і т.п.

1.4.2.2 Класифікація комплексів захисту від спаму

На сьогоднішній день існує величезний вибір всіляких програмних, апаратних та програмно-апаратних комплексів захисту від спаму, розглянемо які є їх види:

1 Комплекси захисту від спаму на безкоштовних поштових службах (gmail.com, i.ua, і т.д.) – алгоритми і системи фільтрації, які розробляють безкоштовні поштові служби. Ці алгоритми вони розробляють на результатах

своєї діяльності, зазвичай це різні чорні, сірі списки та статистичні Баєсовські алгоритми. Зазвичай безкоштовними поштовими службами користуються поодинокі користувачі, або компанії в яких немає власного поштового сервера та які майже не користуються обміном повідомлень через електронну пошту;

2 Безкоштовні програмні комплекси для захисту від спаму - дані комплекси для захисту від спаму, також використовують чорні та сірі списки, статистичну фільтрацію Баєса. Ці комплекси ставляться на внутрішній поштовий сервер підприємства;

3 Платні програмні комплекси для захисту від спаму – в даних комплексах присутні, як стандартні, так нові методики фільтрації, такі як перевірка автентичності на основі IP, виявлення повторів і ознака масовості, фільтрація пошти по ключовим словам;

Таблиця 2.1 – класифікація комплексів захисту від спаму

№	Види програмно апаратних комплексів	Параметри програмно апаратних комплексів												
		Зручність користування	Високий рівень захисту від спаму	Захист конфіденційності почтових повідомлень	Антивірусний захист електронної почти	Захищає від "фітингу;	Автоматичне щомісячне оновлення	Автоматизований чорний список	Інструменти фільтрування по мові повідомлень	Можливість індивідуальних настройок антиспамових фільтрів для окремих груп користувачів	Зменшує загрузку на сервер	Одноразова оплата за послуги	Щомісячна оплата за послуги	Можливість обслуговування необме-женої кількості почтових адресів
1	Комплекси захисту від спаму на безкоштовних почтових службах	-	-	-	-		+	-	-	-	+	-	-	-
2	Безкоштовні програмні комплекси для захисту від спаму.	+	-	+	-	+	-	+	-	-	-	-	-	-
3	Платні програмні комплекси для захисту від спаму	+	+	+	+	+	+	+	+	+	-	-	+	-
4	Програмно-апаратні комплекси	+	+	+	+	+	+	+	+	+	+	+	-	+
5	Програмно апаратні комплекси на зовнішніх серверах.	+	+	-	+	+	+	+	+	+	+		+	-

4 Програмно апаратні комплекси на зовнішніх серверах, які спочатку перевіряють електронну пошту, а потім переправляють на наш сервер, що дозволяє знизити навантаження на поштовий сервер підприємства, але одним із значних не достатків даних комплексів являється те, що оплата за послуги

очистки електронної пошти від спаму та вірусів залежить від кількості поштових адрес, що для великих компаній може бути недоцільно;

5 Програмно апаратні комплекси – це комплекси захисту які мають програмні та апаратні рішення для захисту від спаму. Ці комплекси ставиться на рівні поштового шлюзу в цілях захисту від спаму, фішингових атак, вірусів та іншого шпигунського ПЗ. Одними із основних плюсів даного комплексу становить зниження загрузки з поштового сервера підприємства, високій рівень захисту, та незалежність від кількості поштових адрес та гнучка політика фільтрації.

1.4.3 Розробка методики вибору програмно апаратних комплексів захисту від спаму, по визначеними критеріями підприємств

При виборі засобу захисту від спаму підприємства потрібно класифікувати за наступними параметрами:

1 Цілі використання електронної пошти підприємством і актуальність боротьби зі спамом:

- підприємства на яких використовується один, або декілька електронних адрес і для яких електронна пошта не приносить не доходів, не збитків. На даних підприємствах використовуються безкоштовні поштові сервера і стандартні комплекси захисту які безкоштовно пропонують ці сервера. У разі наявності поштового сервера використовуються безкоштовний спам-фільтр для установки на поштові клієнти Express, Windows Mail, Windows Live Mail і Thunderbird;

- підприємства для яких електронна пошта має рекламний характер і здійснює зв'язок з новими клієнтами, які прийшли від реклами в інтернеті. На цих таких підприємствах доцільно використовувати в залежності від бюджету платні програмні комплекси захисту від спаму, або програмно-апаратні компелекси у вигляді окремого блоку, який ставиться на рівні поштового шлюзу, або програмно-апаратні комплекси зовнішніх серверів;

- підприємства для яких електронна пошта приносить частину доходу (інтернет-магазин). Оскільки на даних підприємствах приноситься дохід від електронної пошти, то до захисту від спаму тут ставляться дуже серйозно і ісльзуют програмно-апаратних комплексів віртуальних серверів, а в разі наявності поштового сервера використовують програмно-апаратні комплекси у вигляді окремого блоку, який ставиться на рівні поштового шлюзу ;
- підприємства на яких електронна пошта використовується для внутрішнього зв'язку;
- підприємства для яких електронна пошта носить інформаційний характер, тобто використовується для відповіді на питання, щодо діяльності підприємства, або установи.

2 Наявність поштового сервера:

- підприємство на яких не використовується поштовий сервер.Цим підприємствам доцільно використовувати безкоштовні поштові сервера і стандартні комплекси захисту які безкоштовно пропонують ці сервера, або використання програмно-апаратних комплексів віртуальних серверів;
- підприємство на яких використовується власний поштовий сервер. Цим підприємствам в залежності від цілей використання електронної пошти доцільно використовувати безкоштовні, або платні спам-фільтр для установки на поштові клієнти Express, Windows Mail, Windows Live Mail і Thunderbird, або використовують програмно-апаратні комплекси у вигляді окремого блоку, який ставиться на рівні поштового шлюзу;

3 Класифікація за кількістю поштових скриньок:

- підприємства на яких використовується кілька поштових адрес. На них в залежності від цілей компанії використання електронної пошти, або від бюджету компанії можна використовувати, абсолютно всі комплекси захисту від спаму;

Таблиця 2.1 – Методика вибору програмно апаратних комплексів захисту від спаму, по визначеними критеріями підприємств

№	Види комолексів захисти від спаму	Параметри підприємств											
		Мета використання електронної пошти					Наявність поштового сервера		Кількість почтових ящиків			Навантаження на сервер	
		В інтересах компанії не використовується	Носить рекламний характер	Приносить прибуток	Використовується для внутрішнього	Носить інформаційний	Не має почтового серверу	Є почтовий сервер.	Декілька	Визначена кількість	Не визначена	Знімає з навантаження	Приносить додаткове на навантаження
1	Комплекси захисту від спаму на безкоштовних поштових службах	+	-	-	-	+	+	-	+	-	-	-	-
2	Безкоштовні програмні комплекси для захисту від спаму.	+	-	-	+	+	-	+	+	+	-	-	+
3	Платні програмні комплекси для захисту від спаму	+	+	+	+	+	-	+	+	+	-	-	+
4	Програмно-апаратні комплекси.	+	+	+	+	+	-	+	+	+	+	+	+
5	Програмно апаратні комолекси на зовнішніх серверах.	+	+	+	+	+	-	+	+	+	-	+	+

- підприємство на яких використовується обмежене число адрес електронної пошти. На них доцільно використовувати платні програмні комплекси захисту від спаму, або використання програмно-апаратних комплексів віртуальних серверів;

- підприємство на яких використовується не обмежена кількість поштових адрес. На цих підприємствах доцільно використовувати програмно-апаратні комплекси у вигляді окремого блоку, який ставиться на рівні поштового шлюзу.

1.4.4 Розробка політики використання електронної пошти для ефективного захисту від спаму

Засіб захисту – система контролю вмісту електронної пошти, само по собі ніяких завдань щодо забезпечення безпеки не вирішує. Це всього лише "машина", яка допомагає людині у вирішенні даної проблеми. Тому завдання по забезпеченню безпеки необхідно такий "машині" поставити. Це означає, що повинен бути вироблений спеціальний звід правил, який надалі буде переведений на мову машини. Такий звід правил називається "політикою використання електронної пошти". [9]

У багатьох організаціях такі правила існують вже тривалий час. Як і всяка обмежувальна міра, вони створюють певні незручності користувачам системи, а якщо користувачеві щось незручно, він або перестає цим користуватися, або намагається обійти перешкоди. Тому такого роду політики, не підкріплені технічними засобами контролю за їх виконанням, поступово втрачають силу. Програмні системи, орієнтовані на фільтрацію пошти, слід позиціонувати саме як інструмент для впровадження і контролю виконання цих правил.

Таким чином, політика використання електронної пошти - це закріплені в письмовому вигляді і доведені до співробітників інструкції та інші документи, які регламентують їх діяльність і процеси, пов’язані з використанням системи електронної пошти. Дані документи та інструкції мають юридичним статусом і, як правило, надаються для ознайомлення співробітникам організації.

Політика використання електронної пошти є найважливішим елементом загальнокорпоративної політики інформаційної безпеки і невіддільна від неї.

Політика повинна відповідати наступним критеріям:

- бути лаконічно викладеною та зрозумілою всім співробітникам компанії, простота написання не повинна привести до втрати юридичного статусу документа;
- виходити з необхідності захисту інформації в процесі економічної діяльності компанії;
- бути узгодженої з іншими організаційними політиками компанії (що регламентують фінансову, економічну, юридичну та інші сфери діяльності компанії);
- мати законну силу, тобто політика, як документ, повинна бути схвалена і підписана всіма посадовими особами керівної ланки компанії, а її виконання має бути детально продумано;
- не суперечити законам України, щодо використання електронної пошти;
- визначати заходи впливу на співробітників, які порушили положення цієї політики;
- дотримувати баланс між ступенем захищеності інформації та продуктивністю діяльності компанії;
- детально визначати заходи щодо забезпечення політики використання електронної пошти в компанії.

Політика використання електронної пошти, як правило, розглядається з двох сторін, як офіційно оформлений юридичний документ і як матеріал, який описує техніку реалізації політики.

Як документ вона повинна включати:

- положення, що електронна пошта є власністю компанії і може бути використана тільки в робочих цілях;
- вказівка на те, що застосування корпоративної системи електронної пошти не повинно суперечити законодавству України і положенням політики безпеки;

- інструкції та рекомендації з використання та зберігання електронної пошти;
- попередження про потенційну відповідальність співробітників компанії за використання електронної пошти в особистих цілях;
- письмове підтвердження того, що співробітники компанії ознайомлені з політикою використання електронної пошти і згодні з її положеннями.

З технічної точки зору політика встановлює правила використання електронної пошти, тобто визначає наступне:

- проходження яких повідомлень вхідної, вихідної або внутрішньої електронної пошти має бути дозволено або заборонено;
- категорії осіб, яким дозволено або заборонено відправляти вихідні або отримувати вхідні повідомлення електронної пошти;
- що необхідно робити з тими чи іншими повідомленнями електронної пошти, які задовольняють або не задовольняють критеріям, визначеним правилами використання електронної пошти.

1.5 Висновок

У розділі були розглянуті загрози корпоративних інформаційних систем пов'язані із зловмисною масовою розсилкою повідомлень.

Захист від спаму має дуже велике значення в корпоративних інформаційних мережах, оскільки за різними джерелами від 70 до 90% електронних повідомлень це неділова кореспонденція, що призводить до таких наслідків:

- зниження продуктивності роботи інформаційної системи;
- відчутне зниження продуктивності праці у персоналу організації, через очищення поштових скриньок від спаму;
- перехід за посиланнями на розважальні ресурси, що згодом впливає на трудову активність персоналу і доходи організації;
- значне збільшення часу пошуку потрібних листів або інформації;

- зниження працездатності або ж відмова в обслуговуванні поштової системи і поштових серверів через великого потоку даних;
- "фішинг" – вид інтернет-шахрайства, при якому зловмисник змушує користувача виконати певні дії шляхом відправки листів жертві від імені довіреного відправника;
- загромадження ресурсів інформаційної системи (заняття дискового простору під неділову пошту).

В кінцевому результаті була розроблена методологія захисту корпоративних інформаційних систем від спаму, яка складається з організаційних та програмно-апаратних заходів.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальна характеристика підприємства

Фірма “Фотон” займає вигідне географічне положення, на перетині залізничних та автомобільних магістралей. Історія фірми починається з 1992 року, коли вийшла її перша продукція, а згодом і почала користуватись попитом у українських і зарубіжних споживачів. З часом розширення технічних, фінансових і фахових чинників та мережі збуту продукції, дало можливість створити сучасне виробництво, відкрити нові технічно обладнані виробничі цехи, склад-магазин, нове офісне приміщення та інші складові забезпечення діяльності підприємства.

Тепер підприємство виробляє декоративні та господарські вироби з металу, вікна з натурального брусу, проводить торгівлю власними виробами та для забезпечення належної діяльності підприємства, та з метою забезпечення конкурентоспроможності продукції на вітчизняних та іноземних ринках, створена сучасна технічна і технологічна база, виробнича та соціальна інфраструктура, проводиться навчання та стажування персоналу і фахівців фірми. Широко використовується співпраця із закордонними фірмами, здебільшого, як обмін ідеями, вивченням сучасних технологій та в рекламній галузі. Налагоджено ділову співпрацю з іноземними партнерами в тому числі резидентами Франції, Німеччини, Італії, Польщі, Португалії, Білорусі.

Предметом діяльності Товариства є:

- закупівля, розробка та реалізація сільськогосподарської продукції;
- виробництво продукції виробничо-технічного призначення та товарів народного споживання як промислової так і продовольчої групи;
- здійснення ремонтно-будівельних, монтажних та підрядних робіт;
- надання транспортно-експедиційних послуг при перевезеннях зовнішньо-торгівельних і транзитних вантажів;

- оптова, роздрібна, комісійна (в т.ч. скупка) торгівля продукцією та товарами;
- надання посередницьких, маркетингових консультаційних, брокерських, дилерських, дистриб'юторських, рекламних та інших послуг не заборонених законодавством;
- надання консультаційних, аудиторських, сервісних послуг;
- проведення бартерних операцій;
- проведення торгів, аукціонів, конкурсів;
- виробництво та переробка продуктів харчування (включаючи дитяче);
- брокерська діяльність на біржах;
- зовнішньоекономічна діяльність, експорт та імпорт обладнання, сировини та матеріалів, енергоресурсів, технологічної документації, приладів, комплектуючих виробів, машин та механізмів, товарів народного вжитку;
- здійснення міжнародних та внутрішніх перевезень пасажирів і вантажів автомобільним транспортом;
- купівля, продаж, обмін іноземної валюти;
- будівництво та ремонт об'єктів промислового соціально-економічного та житлового призначення;
- виробництво будівельних матеріалів;
- ремонт та сервісне обслуговування автомобілів та побутової техніки;
- організація та отримання відеосалонів, дискотек, барів, кафе та інших закладів громадського харчування;
- надання туристичних та готельних послуг;
- надання митно-брокерських послуг;
- організація виставок та ярмарок;
- організація курсів та навчальних закладів;
- лізингові та орендні операції з рухомим майном;
- здійснення фармацевтичної та лікувально-профілактичної діяльності;

- медична практика;
- видавнича діяльність;
- надання побутових послуг населенню;
- інші види діяльності, що не заборонені законодавством України.

Підприємство “Фотон” постійно нарощує об’єми виробництва та реалізації продукції, розширює асортимент своїх виробів, впроваджує нові технології, тісно співпрацює з іноземними партнерами, а також з фірмами в межах України.

Штат співробітників включає 18 осіб. З них:

- директор;
- секретар;
- бухгалтер;
- менеджери по збуту - 5 чол.;
- адміністратор - 1 чол.;
- вантажники - 5 чол.;
- охорона - 3 чол.;
- прибиральниця.

2.2 Класифікація інформаційної системи підприємства «Фотон»

Критерії оцінки захищеності інформаційної системи є методологічною базою для визначення вимог захисту інформації в комп’ютерних системах від несанкціонованого доступу; створення захищених комп’ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп’ютерних системах та їх придатності для обробки критичної інформації.[13]

Критерії надають:

а) порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп’ютерних системах;

б) базу (орієнтири) для розробки комп’ютерних систем, у яких повинні бути реалізовані функції захисту інформації.

Функціональні критерії розбиті на три групи, кожна з яких описує вимоги до послуг, які забезпечують захист від загроз одного з чотирьох основних типів:

1 Конфіденційність. Загрози, які відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності;

2 Цілісність. Загрози, які відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності;

3 Доступність. Загрози, які відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

Категорії доступності:

- критична – без неї робота суб'єкта зупиняється (ДО);
- дуже важлива – без неї можна працювати, але дуже короткий час (Д1);
- важлива – без неї можна працювати деякий час, але з часом вона знадобиться (Д2);
- корисна – без неї можна працювати, але її використання заощаджує ресурси (Д3);
- несуттєва – застаріла або невживана, що не впливає на роботу суб'єкта (Д4).

Категорії цілісності:

- критична – її несанкціонована зміна призведе до неправильної роботи всього суб'єкта або значної його частини; наслідки модифікації незворотні (Ц0);
- дуже важлива – її несанкціоноване зміна призведе до неправильної роботи суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки модифікації незворотні (Ц1);
- важлива – її несанкціоноване зміна призведе до неправильної роботи частини суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки модифікації оборотні (Ц2);

- значна – її несанкціоноване зміна позначиться через деякий час, але не призведе до збою в роботі суб'єкта; наслідки модифікації оборотні (Ц3);
- незначна – її несанкціонована зміна не позначиться на роботі системи (Ц4).

Категорії конфіденційності:

- критична – розголошення інформації призведе до краху роботи суб'єкта або до дуже значних матеріальних втрат (КО);
- дуже важлива – розголошення призведе до значних матеріальних втрат, якщо не будуть зроблені деякі дії (К1);
- важлива – розголошення призведе до деяких матеріальним (можебути, непрямим) або моральних втрат, якщо не будуть зроблені деякі дії (К2).
- значна – приносить скоріше моральний збиток, може бути використана тільки в певних ситуаціях (К3);
- малозначима – може принести моральну шкоду в дуже рідкісних випадках (К4).

Таблиця 2.1 – Класифікація об'єктів підприємство «Фотон»

ПК	Доступність	Цілісність	Конфіденційність
Директор	Д2	Ц1	К0
Секретар	Д3	Ц2	К1
Бухгалтера	Д1	Ц1	К1
Менеджери зі збуту	Д1	Ц1	К1
Адміністратор	Д1	Ц1	К1

2.3 Аналіз комплексної системи захисту інформації підприємства «Фотон»

Для захисту інформаційних ресурсів на підприємстві функціонує комплексна система захисту інформації, яка включає в себе:

- підсистема управління доступом. Передбачає захист інформаційних ресурсів від несанкціонованого доступу. Засобами підсистеми реалізуються функції з управління доступом користувачів до ресурсів, включаючи мережеві підключення і доступ до зовнішніх носіїв інформації та пристроїв;
- підсистема реєстрації та обліку. Передбачає захист інформаційних ресурсів Замовника від несанкціонованого доступу. Засобами підсистеми реалізується реєстрація та облік дій користувачів в різних системах, що дозволяє, наприклад, зафіксувати факти звернення користувачів до конфіденційних ресурсів;
- підсистема забезпечення цілісності. Дозволяє запобігати підміну справжнього програмного середовища на модифіковане як зловмисником, так і в результаті системних збоїв;
- підсистема криптографічного захисту. Забезпечує захист даних при зберіганні і передачі по каналах зв'язку. Підсистема включає в себе засоби формування ЕЦП;
- підсистема забезпечення мережевої безпеки. Запобігає можливі атаки, реалізовані на мережевому рівні. Включає в себе засоби міжмережевого екранування, організації захищених віртуальних мереж (включаючи віддалених користувачів);
- підсистема контролю використання інформаційних ресурсів. Запобігає витоку інформації через канали зв'язку, носії інформації, USB, Bluetooth, CD / DVD . Може передбачати обмеження нецільового використання співробітниками ресурсів організації, в тому числі ресурсів Інтернет, електронної пошти та мережевих ресурсів;
- підсистема забезпечення безперервності функціонування Комплексної системи захисту інформації. Забезпечує безперебійну роботу засобів захисту інформації при різних нештатних ситуаціях;
- підсистема управління обліковими записами. Передбачає захищене централізоване управління обліковими записами користувачів. Включає надання

користувачу ролей для доступу до різних систем, а також перевірку і коригування надмірності прав користувачів. В рамках даної підсистеми реалізується централізоване управління засобами захисту інформації, що включає управління оновленнями, а також повідомлення адміністраторів про інциденти інформаційної безпеки;

- підсистема контролю захищеності. В рамках даної підсистеми проводиться інвентаризація інформаційних ресурсів організації, аналіз загроз та інформаційних ризиків, інструментальний аналіз захищеності інфраструктури, контроль виконання політик безпеки. Результатом є оцінка поточного рівня захищеності інформаційно-обчислювальної системи Замовника та виконання заходів з підвищення рівня захищеності.

Зробивши аналіз комплексної системи захисту інформації підприємства «Фотон» видно що дана система не має ніяких засобів захисту від загроз пов'язаних із злоякісною масовою розсилкою повідомлень, що призводить до наступних наслідків:

- зниження продуктивності адміністратора мережі;
- зниження продуктивності працівників підприємства, через трату часу на обробку не ділової кореспонденції.

2.4 Аналіз програмного забезпечення для використання електронної пошти на підприємстві «Фотон»

В якості поштового сервера використовується Microsoft Exchange 2003, що володіє наступними особливостями:

- MS Exchange 2010 працює спільно з MS Windows 2008 Server, розроблений як засіб спілкування та співпраці для бізнесу будь-якого розміру. Разом з MS Outlook 2010, MS Exchange 2010 представляє високонадійну, масштабовану і легку в управлінні інфраструктуру для спільної роботи та обміну повідомленнями [14];

- MS Exchange 2010 Server надає великі можливості для організації різних видів спільної роботи, включаючи можливості групового планування, дискусійні групи та організацію командної роботи з документами за допомогою спеціалізованих папок поштового сервера. Вбудована технологія індексування і пошуку інформації дозволяє користувачам швидко знаходити і розділяти інформацію;
- Можливий доступ до пошти, адресної книги, контактів з будь-якого виду пристроїв персональний комп'ютер, ноутбук, кишеньковий комп'ютер, мобільний телефон. Сервер сам визначає вигляд пристрою і висилає інформацію у відповідному форматі в результаті чого, інформацію зручно сприймати на будь-якому пристрої;

Досить важливу роль у функціонуванні підприємства відіграє електронна пошта, через яку здійснюються наступні операції:

- здійснюється зв'язок з потенційними клієнтами;
- здійснюється продаж товарів;
- надається інформація про наявність товарів;
- висилаються цінники по товарам;
- надається інформація про нові надходження,та про нові види товарів.

2.4.1 Аналіз загроз електронної пошти підприємства «Фотон» пов'язаних із зловмисною масовою розсилкою повідомлень

Поява не ділової кореспонденції призводить до наступних загроз:

- переповнення буфера в Microsoft Outlook Express, що дозволяє віддаленому зловмисникові виконати шкідливий програмний код. Уразливість існує через помилку в перевірці вхідних даних при обробці NNTP відповідей. Атакуючий може передати спеціально сформовані NNTP відповіді, що призведе до виконання довільного коду;
- переповнення буфера в Microsoft Windows Mail і Outlook Express. Уразливість дозволяє віддаленому зловмисникові виконати шкідливий

програмний код. Уразливість існує через помилку в перевірці вхідних даних в NNTP клієнтів Microsoft Windows Mail і Outlook Express. Атакуючий може обманним чином заманити користувача на спеціально складений сайт, що призведе до виконання довільного коду;

- порушення доступності інформації в Outlook Express при обробці повідомлень;
- зниження продуктивності адміністратора мережі;
- зниження продуктивності працівників підприємства, через трату часу на обробку не ділової кореспонденції;
- паразитний поштовий трафік;
- появи помилок першого та другого роду, під час виявлення надійності поштових повідомлень.

2.5 Розробка системи захисту від загроз пов'язаних із зловмисною масовою розсилкою повідомлень

2.5.1 Вибір комплексу захисту від спаму для підприємства «Фотон», згідно розробленої методики

Вибір комплексу захисту від загроз пов'язаних із зловмисною масовою розсилкою повідомлень був здійснений за допомогою розробленої методики.

В цій методиці вибір комплексу захисту від спаму, залежить від параметрів підприємства, таких, як мета використання електронної пошти, наявність поштового сервера, кількість поштових адрес і загрузки на поштовий сервер.

Згідно цієї методики, для захисту від спаму на підприємстві «Фотон» найбільш доцільно буде використовувати програмно-апаратні комплекси на зовнішніх серверах. Цей вибір обґрунтовується наступними критеріями:

- використання електронної пошти носить рекламний та інформаційний характери, тобто через неї здійснюється зв'язок з

потенціальними покупцями, інформуються клієнти про нові надходження товару і даються відповіді на запитання клієнтів про характеристики продукції;

Таблиця 2.2 – Методика вибору програмно апаратних комплексів захисту від спаму, по визначеними критеріями підприємств

	Види комплексів захисти від спаму	Параметри підприємств											
		Мета використання електронної пошти					Наявність поштового сервера		Кількість поштових адрес			Навантаження на сервер	
		В інтересах компанії не використовується	Носить рекламний характер	Приносить прибуток	Використовується для внутрішнього зв'язку	Носить інформаційний характер	Не має поштового серверу	Є поштовий сервер.	Декілька	Визначена кількість	Не визначена кількість	Знімає навантаження з сервера	Приносить додаткове навантаження на сервер
1	Комплекси захисту від спаму на безкоштовних поштових службах	+	-	-	-	+	+	-	+	-	-	-	-
2	Безкоштовні програмні комплекси для захисту від спаму.	+	-	-	+	+	-	+	+	+	-	-	+
3	Платні програмні комплекси для захисту від спаму.	+	+	-	+	+	-	+	+	+	-	-	+
4	Програмно-апаратні комплекси.	+	+	+	+	+	-	+	-	-	+	+	+
5	Програмно-апаратні комплекси на зовнішніх серверах.	+	+	+	+	+	-	+	+	+	-	+	+

- в якості поштового сервера використовується Microsoft Exchange ;
- на підприємстві «Фотон» сім поштових адрес, що дозволяє заощадити кошти компанії;
- оскільки на підприємстві великий потік електронної пошти, то доцільно знизити навантаження на поштовий сервер.

Оцінивши програмно-апаратні комплекси на зовнішніх серверах,було здійснено вибір служби Microsoft Forefront Online Security for Exchange.

Цей вибір обґрунтовується за наступними параметрами:

- дешевизна сервісу, оскільки послуги оплачуються за кожний окремий поштовий адрес;
- легкість адміністрування, оскільки дана служба була розроблена спеціально для поштових серверів Microsoft Exchange;
- гнучка політика фільтрації, що дозволяє створити різні правила користування та фільтрації електронної пошти.

Також даний вибір обґрунтовується тим що компанія Microsoft гарантує:

- точність політики фільтрації;
- виявлення і блокування вірусів – 100 відсотковий захист від усіх відомих вірусів електронної пошти;
- блокування 98% вхідної небажаної пошти;
- помилкових спрацьовувань - менше 1 на 250000 повідомлень електронної пошти;
- час безвідмовної роботи мережі - 99,999%;
- доставка електронної пошти - середній час доставки складає менше однієї хвилини.

2.5.2 Характеристика служби Microsoft Forefront Online Security for Exchange

Служба Microsoft Forefront Online Security for Exchange – це повністю автоматизована, служба фільтрації електронної пошти, яка допомагає захистити

організацію від небажаної пошти, шкідливих програм. [14]

Сервіс Microsoft Forefront Online Security for Exchange захищає середовище обміну повідомленнями шляхом фільтрації вхідної пошти до її надходження в поштову систему. Служба Microsoft Forefront Online Security for Exchange отримує всі вхідні повідомлення, перевіряє на небажану пошту і віруси, застосовує фільтри захисту від небажаної пошти і передає пошту в середовище обміну повідомленнями для подальшої перевірки та доставки на поштовий сервер підприємства.

Оскільки цей сервіс видаляє з поштових повідомлень спам і віруси, ще до того як вони попадають у корпоративну мережу компанії, то це зменшує обсяг поштового трафіку, що дозволяє знизити вартість оплати підключення до Internet. Крім того вона спрощує управління поштовим середовищем, а також обслуговування програмного забезпечення і устаткування та дозволяє зняти з компанії навантаження на власні поштові сервери.

Саме рішення не вимагає великого впровадження - досить переналаштувати маршрутизацію пошти, що приходить на певний домен, так, щоб її спочатку обробляли сервери хостинг-центру Microsoft. Після того як пошта очищається, вона через між мережевий екран передається на внутрішній сервер компанії, побудований на базі Microsoft Exchange. Далі листи стають доступи користувачам усередині корпоративної мережі.

Служба Microsoft Forefront Online Security for Exchange – це глобальна мережа центрів обробки даних, яка створена на основі відмовостійкої і розгалуженої архітектури, що забезпечує балансування навантаження між мережами і всередині кожного центру обробки даних. Центри обробки даних розташовані по всьому світу. Якщо центр обробки даних раптово стане недоступний, трафік буде автоматично перенаправлено на інший центр обробки даних без переривання роботи служби. Тисячі поштових серверів цієї служби беруть електронну пошту від імені вашої організації, розділяючи сервери організації та Інтернет. Для забезпечення своєчасної та ефективної доставки,

алгоритми створені корпорацією Майкрософт, аналізують і перенаправляють сполучення між центрами обробки даних. Завдяки такій високій доступності мережі, корпорація Майкрософт може забезпечувати час безперебійної роботи на рівні 99,999%. Цей метод, заснований на моделі розподіленого сервера та програмного забезпечення, показав добрі результати захисту корпоративних мереж і поштових серверів організацій від найбільш поширених загроз, таких як небезпечні віруси, атаки типу "відмова в обслуговуванні", атаки з метою збору діючих адрес, атаки перебором по словнику та інші види застосування електронної пошти не за призначенням.

Служба Microsoft Forefront Online Security for Exchange блокує до 98% небажаної пошти, а її багаторівнева архітектура ефективно перевіряє решту 2% електронної пошти на наявність шкідливих програм до того, як вони потраплять на поштові сервери організації.

2.5.2.1 Алгоритми фільтрації електронної пошти в Microsoft Forefront Online Security for Exchange

Фільтрація електронної пошти в Microsoft Forefront Online Security for Exchange, відбувається за допомогою стандартних та додаткових методів фільтрації. [16]

До стандартних методів фільтрації відносяться:

а) чорні списки. Поштові та IP-адреси, з яких розсилається спам, вносяться в чорні списки і блокуються на рівні провайдерів або самим користувачем. Завдяки простоті реалізації використання цих black-листів проводиться через службу DNS.I цей метод в силу ряду причин стає все менш ефективним, зате призводить до порушення цілісності Мережі, коли цілком добропорядні користувачі втрачають можливість вести свою переписку;

б) сірі списки. Принцип дії сірих списків заснований на тактиці розсилки спаму. Як правило, спам розсилається в дуже короткий час у великій кількості з якого-небудь сервера. Робота сірого списку полягає в навмисній затримці отримання листів на деякий час. При цьому адреса і час пересилки

заноситься в базу даних сірого списку. Якщо віддалений комп'ютер є справжнім поштовим сервером, то він повинен зберегти лист у черзі і повторювати пересилання протягом п'яти днів. Спам-боти, як правило, листів в черзі не зберігають, тому через нетривалий час, припиняють спроби переслати листа;

в) фільтрація пошти по ключовим словам. Ефективність цього методу дуже низька, оскільки вимагає великих витрат на створення і підтримку бази ключових слів. Крім того, спамери постійно винаходять нові і нові способи обійти подібні фільтри. Наприклад, в російськомовних листах використовується прийом підміни російських букв латинськими, подібними з написання (а, е, В, в і так далі);

г) запит на підтвердження. Перш ніж показати лист одержувачу, генерується запит його відправникові: підтвердіть, що ви дійсно писали повідомлення такого-то і такому-то. Якщо відправник підтверджує факт написання листа, він визнається "не спамером" і його адресу вноситься в білий список. З цього моменту пошта від нього до одержувача проходить без проблем. Але цей метод фільтрації також не позбавлений очевидних недоліків. По-перше, він доставляє масу незручностей "не спамерам", по-друге, багато спамери вже цілком здатні генерувати листи-підтвердження, що зводить нанівець переваги даного способу фільтрації, і призводить до ще більшого збільшення паразитного трафіку;

д) статистична фільтрація. Найбільш перспективними, на сьогоднішній день виглядають рішення, засновані на статистичній фільтрації вхідної пошти. В основу їх роботи покладена теорема Байеса, яка оцінює ймовірність настання якої-небудь події виходячи зі статистики вчинення цього ж події в минулому. Наприклад, якщо користувач зустрів слово телемагазин в дев'яти спамерських посланнях і лише в одному "чистому" листі, то у нього з'являється можливість оцінити, з якою ймовірністю наступний лист, що містить слово телемагазин, буде спамом;

е) статистичні Байєсовські алгоритми призначені для аналізу контенту.

Байєсовські фільтри не потребують постійної налаштування. Все, що їм потрібно - це попереднє навчання. Після цього фільтр підлаштовується під тематики листів, типові для даного конкретного користувача. Тим самим, якщо користувач працює в системі освіти і проводить тренінги, то особисто у нього повідомлення даної тематики не будуть розпізнаватися як спам. У тих, кому пропозиції відвідати тренінг не потрібні, статистичний фільтр віднесе такі повідомлення до спаму;

ж) виявлення повторів і ознака масовості. Якщо антиспамовий система має справу з великим потоком листів, вона може і повинна намагатися знаходити повтори листів. По-перше, так можна виловлювати листи, вже відомі (помічені раніше) як спам. По-друге, масовість листи сама по собі є невід'ємною ознакою спаму. З твердження, що лист є спам, неминуче випливає, що воно масове. Таким чином, ознака масовості є необхідна, хоча і не достатня умова спаму. Для побудови працездатного «масового» аналізатора потрібні величезні потоки пошти, тому цю технологію пропонують великі виробники, що володіють значними обсягами пошти, яку вони можуть піддати аналізу;

Після проходження стандартних методів фільтрації повідомлення має пройти наступні чотири додаткових рівня технології захисту від небажаної пошти:

а) перевірка автентичності на основі IP. Служба Microsoft Forefront Online Security for Exchange перевіряє справжність ідентифікатора відправника кожного повідомлення електронної пошти. Якщо справжність повідомлення не вдається перевірити і буде встановлено, то повідомлення, швидше за все, буде відзначено як небажане. Інфраструктура політики відправників - галузевий стандарт, який запобігає підробку зворотних адрес, використовуючи ідентифікатор відправника SMTP-пошти в повідомленнях, що полегшує ідентифікацію підробок. Уточнюючий запит інфраструктура політики відправників допомагає підтвердити, що об'єкт, зазначений як відправник, насправді відправив повідомлення електронної пошти;

б) дактилоскопія. Коли повідомлення містять відомі характеристики небажаної пошти, вони ідентифікуються і "дактилоскопіюється", тобто отримують унікальний ідентифікатор на основі їх вмісту. База даних збирає відомості про всіх відправників небажаних повідомлень, блокованих системою Microsoft Forefront Online Security for Exchange, що покращує і вдосконалює процес їх "дактилоскопірування" у міру обробки нових повідомлень. Коли повідомлення з певними "відбитками" проходить через систему вдруге, "відбитки" знімаються і повідомлення позначається як небажане. Система постійно аналізує вхідні повідомлення, щоб виявити нові методи розсилки спаму. Група аналітиків небажаної пошти служби Microsoft Forefront Online Security for Exchange оновлює рівень "відбитків", коли визначаються нові методи;

в) підрахунок балів на основі правил. Служба Microsoft Forefront Online Security for Exchange присвоює бали повідомленнями, яких в системі більш як 20 000, які втілюють і визначають характеристики небажаних і надійних повідомлень електронної пошти. Бали нараховуються, якщо повідомлення містить характеристики небажаного повідомлення, і знімаються, якщо повідомлення містять характеристики надійних повідомлень електронної пошти. Коли кількість балів для повідомлення перевищує певний максимум, повідомлення позначається як небажане.

Служба Microsoft Forefront Online Security for Exchange оцінює і нараховує бали за наступні характеристики повідомлень:

- фрази в тексті і рядку теми повідомлення, включаючи URL-адреси;
- заплутування протоколу HTTP в спробі представити URL-адресу небажаної пошти як надійний URL-адресу;
- неправильно побудовані заголовки;
- вид поштового клієнта;
- створення заголовків, наприклад, "Ідентифікатор повідомлення", "Отримано", випадкові символи;

- вихідний поштовий сервер;
- вихідний поштовий агент;
- адреса відправника й адреса відправника SMTP.

Робоча група по роботі з небажаною поштою в міру необхідності змінює чинні і додає нові правила кілька разів на день.

2.5.3 Впровадження служби захисту від спаму Microsoft Forefront Online Security for Exchange на підприємстві «Фотон»

Для того щоб користуватися послугами Microsoft Forefront Online Security for Exchange необхідно:

а) необхідно зайти на сайт Microsoft Forefront Online Security for Exchange і зареєструвати обліковий запис;

б) необхідно включити управління шлюзом Microsoft Forefront Online Security for Exchange, ввести облікові дані адміністратора домену для сервера шлюзу і облікові дані Microsoft Forefront Online Security for Exchange, створені при реєстрації в Microsoft Forefront Online Security for Exchange, і завантажити IP-адреси для центру даних Microsoft Forefront Online Security for Exchange, щоб оновити параметри брандмауера і з'єднувачів отримання Exchange. Якщо інтернет трафік проходить через проксі-сервер, також необхідно ввести параметри проксі-сервера, щоб шлюз Microsoft Forefront Online Security for Exchange міг підключитися до Інтернету;

в) після реєстрації в Microsoft Forefront Online Security for Exchange та налаштування параметрів, необхідно перенаправити всю вхідну пошту в центр даних Microsoft Forefront Online Security for Exchange, змінивши записи MX таким чином, щоб вони вказували на центр даних Microsoft Forefront Online Security for Exchange. Також необхідно змінити правила брандмауер и параметри внутрішнього поштового серверу Exchange таким чином, щоб дозволити отримання пошти лише з серверів Microsoft Forefront Online Security for Exchange.

2.5.4 Розробка організаційних методів захисту від загроз пов'язаних із зловмисною масовою розсилкою повідомлень

Суть організаційних методів захисту від загроз пов'язаних із зловмисною масовою розсилкою повідомлень, заключається в розробці та впровадженні політики користування електронною поштою.

Ця політика визначає правила використання корпоративної електронної пошти в компанії.

Ця політика регламентує такі правила:

1 Співробітнику забороняється:

- використовувати корпоративну електронну пошту для розсилки матеріалів екстремістського, расистського, порнографічного та кримінального характеру;
- використовувати корпоративну електронну пошту для здійснення масової розсилки електронної кореспонденції;
- використовувати ящики електронної пошти, створені на зовнішніх Інтернет-ресурсах таких як www.gmail.com і т.п. для виконання посадових обов'язків;
- пересилати виконувані файли (з розширенням. Exe,. Com,. Jar,. Msi,. Bat);
- пересилати на зовнішні адреси електронної пошти конфіденційні дані без застосування засобів шифрування;
- пересилати повідомлення, що містять вкладення, розмір яких перевищує 10 Мб;
- використовувати обліковий запис іншого співробітника для пересилання повідомлень від чужого імені;
- пересилати «листи-щастя», що містять прохання про пересилання іншим адресатам.

2 Співробітникові не рекомендується:

- переходити за посиланнями в листах з ненадійних джерел;

- при відповіді на лист, що містить вкладення, залишати їх в тілі повідомлення в разі відсутності в цьому явної необхідності;
- пересилати повідомлення з порожньою темою листа;
- включати адресатів в полі "прихована копія";
- змінювати чиєсь електронне повідомлення без чіткої вказівки того, яка частина повідомлення було змінено.

3 Співробітникові рекомендується:

- регулярно перевіряти електронну пошту (не рідше, ніж кожні півгодини);
- бути ввічливим;
- з акуратністю користуватися опцією «відповісти всім» для виключення можливості пересилання повідомлення помилковим адресатам;
- в разі, якщо відсутня можливість перевірити електронну пошту протягом більш ніж одного робочого дня, використовувати функцію автовідповіді із зазначенням альтернативних засобів зв'язку;
- регулярно переміщати вхідні та вихідні листи в локальний поштовий архів;
- у разі якщо автор листа звертається до адресата з проханням вжити якісь дії, що тягнуть за собою передачу таких даних: ім'я облікового запису користувача, пароль, персональні дані співробітника (ім'я, прізвище, номер паспорта, дата народження, адреса), номер кредитної карти, вжити необхідні дії для з'ясування достовірності відправника листа і правомірності подібного прохання.

2.6 Висновок

Уданій частині роботи були розглянута комплексна система захисту інформації підприємства «Фотон». Та було впроваджено на даному підприємстві система захисту електронної пошти від загроз пов'язаних із масовою розсилкою повідомлень.

В якості програмно-апаратного комплексу захисту від спаму було обрано Microsoft Forefront Online Security for Exchange.

Даний вибір обґрунтовується тим що компанія Microsoft гарантує:

- точність політики фільтрації;
- виявлення і блокування вірусів – 100 відсотковий захист від усіх відомих вірусів електронної пошти;
- блокування 98% вхідної небажаної пошти;
- час безвідмовної роботи мережі - 99,999%;
- доставка електронної пошти - середній час доставки складає менше однієї хвилини.

Також були розроблені організаційні заходи для захисту підприємства «Фотон» від загроз пов’язаних із зловмисною масовою розсилкою повідомлень.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності розробки засобів захисту інформаційно-комунікаційної системи підприємства «Фотон» від зловмисної масової розсилки повідомлень. Обґрунтування економічної доцільності передбачає здійснення розрахунку капітальних та експлуатаційних витрат, визначення величини економічного ефекту, а також показників економічної ефективності щодо запропонованих рішень.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні (фіксовані) витрати визначаються величиною коштів, призначених для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Визначення витрат на підвищення рівня інформаційної безпеки підприємства шляхом розробки заходів захисту корпоративної інформаційної систем від спаму

3.1.1.1 Визначення трудомісткості розробки заходів захисту корпоративної інформаційної системи від спаму

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$T = t_{тз} + t_в + t_а + t_р + t_д, \text{ годин},$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку заходів захисту корпоративної інформаційної систем від спаму, $t_{тз}=20$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=32$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=40$;

$t_р$ – тривалість розробки засобів захисту корпоративних інформаційних систем від спаму, $t_м=64$;

$t_д$ – тривалість підготовки технічної документації, $t_д=12$.

Отже,

$$t = 20+32+40+64+12 = 168 \text{ годин}.$$

3.1.1.2 Розрахунок витрат на підвищення рівня інформаційної безпеки підприємства шляхом розробки заходів захисту корпоративної інформаційної систем від спаму

Витрати на розробку заходів безпеки Кпз складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 25872 + 2491,44 = 28363,44 \text{ грн}.$$

$$З_{зп} = t\ З_{пр} = 168*154 = 25872 \text{ грн.}$$

де t – загальна тривалість операцій, годин;

Зпр – средньогодинна заробітна плата спеціаліста с інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{Мч} = t \cdot С_{Мч} = 168 \cdot 14{,}83 = 2491{,}44 \text{ грн.}$$

де t – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{Мч} = 0{,}8 \cdot 11 \cdot 1{,}55 + \frac{8600 \cdot 0{,}3}{1920} + \frac{5200 \cdot 0{,}4}{1920} = 14{,}83 \text{ грн.}$$

При розробці заходів із забезпечення кібербезпеки через захист корпоративних інформаційних систем від спаму планується розробка організаційних та програмно-апаратних заходів. На підприємстві «Фотон» вже існує наявне апаратне забезпечення, тому капітальні витрати у зв'язку з його закупівлею не виникають.

В результаті проведеного порівняння програмно-апаратних комплексів на зовнішніх серверах для вирішення завдань захисту інформаційно-комунікаційної системи підприємства «Фотон» від зловмисної масової розсилки повідомлень обрано служби Microsoft Forefront Online Security for Exchange. Вартість такого програмного забезпечення складає 2692 грн. для необмеженої кількості робочих станцій.

Планується здійснення витрат на навчання технічних фахівців і обслуговуючого персоналу, які складуть 3000 грн. ($К_{навч}$=3000 грн.), а також витрати на налагодження системи інформаційної безпеки в розмірі 6000 грн. ($К_н$=6000 грн.)

Отже, капітальні (фіксовані) витрати на підвищення рівня інформаційної безпеки підприємства шляхом розробки заходів захисту корпоративної інформаційної систем від спаму складуть:

$$К = 28363,44 + 2692 + 3000 + 6000 = 40055,44 \text{ грн.}$$

3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.}$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки).

При розробці заходів захисту корпоративної інформаційної систем від спаму виникають витрати подовження дії ліцензії програмного забезпечення Microsoft Forefront Online Security for Exchange, які складають 248 грн./місяць. Відповідно, річні витрати на відновлення та модернізацію системи складуть:

$$С_в = 248*12 = 2976 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 15600 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Отже,

$$С_з = 15600*12 + 15600*12*0,08= 202176 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 202176*0,22 = 44478,72 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=6,2 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 6,2*1920*1,55 = 18451,2 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 40055,44*0,01=400,55 грн).

Оскільки сервіс Microsoft Forefront Online Security for Exchange видаляє з поштових повідомлень спам і віруси, ще до того як вони попадають у корпоративну мережу компанії, то це зменшує обсяг поштового трафіку, що дозволяє знизити вартість оплати підключення до Internet. Планове зниження витрат на підключення до Internet складає 255 грн.

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 202176 + 44478,72 + 18451,2 + 400,55 – 255 = 265271,47 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 2976 + 265271,47 = 268247,47 \text{ грн.}$$

3.2 Оцінка можливого збитку

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 5 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 10 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 16000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 9 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 800 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 52.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{15000 \cdot 9}{176} \cdot 2 = 1534{,}09 \quad \text{грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{15000 \cdot 9}{176} \cdot 10 = 7670{,}45 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{16000 \cdot 1}{176} \cdot 5 = 454{,}54 \text{ грн.}$$

Таким чином, витрати на відновлення працездатності вузла або сегмента корпоративної мережі складають:

$$Пв = 7670{,}45+454{,}54= 8124{,}99 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}) = \frac{800000}{2080} \cdot (2+5+10) = 6538{,}46 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 1534{,}09 + 8124{,}99 + 6538{,}46 = 16197{,}54 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \Sigma_i \Sigma_n U = \Sigma_1 \Sigma_{50} 16197{,}54 = 809877 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (R=0,4);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 809877*0,4 - 268247,47 = 55703,33 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{55703,33}{40055,44} = 1,39, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (5,5 %);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,39 > (5,5 - 5)/100 = 1,39 > 0,005.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Відповідно термін окупності розробки заходів захисту web-додатків від інформаційних атак на основі java-аплетів:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,39} = 0,72, \quad \text{років (8,64 місяця).}$$

3.4 Висновок

Згідно з наведеними розрахунками можна зробити висновок, що розробку заходів захисту корпоративної інформаційної систем від спаму можна вважати економічно доцільною, оскільки вживання таких заходів передбачає отримання економічного ефекту у розмірі 1,39 грн. на 1 грн. капітальних вкладень (ROSI=1,39). Термін окупності при цьому складе 0,72 року або 8,64 місяці. Щорічні експлуатаційні витрати плануються на рівні 268247,47 грн.

ВИСНОВКИ

Захист від спаму має дуже велике значення в корпоративних інформаційних мережах, оскільки за різними джерелами від 70 до 90% електронних повідомлень це неділова кореспонденція, що призводить до таких наслідків:

- зниження продуктивності роботи інформаційної системи;
- відчутне зниження продуктивності праці у персоналу організації, через очищення поштових скриньок від спаму;
- перехід за посиланнями на розважальні ресурси, що згодом впливає на трудову активність персоналу і доходи організації;
- значне збільшення часу пошуку потрібних листів або інформації;
- зниження працездатності або ж відмова в обслуговуванні поштової системи і поштових серверів через великого потоку даних;
- "фішинг" – вид інтернет-шахрайства, при якому зловмисник змушує користувача виконати певні дії шляхом відправки листів жертві від імені довіреного відправника;
- загромадження ресурсів інформаційної системи (заняття дискового простору під неділову пошту).

У роботі була дослідження і розробка методології захисту корпоративних інформаційних систем від загроз пов’язаних із зловмисною масовою розсилкою повідомлень, подальшим впровадженням цієї методики на підприємстві «Фотон».

В економічному розділі виконано розрахунок економічного ефекту від впровадження розроблених методів захисту корпоративних інформаційних систем від загроз пов’язаних із масовою розсилкою повідомлень на підприємстві «Фотон».

ПЕРЕЛІК ПОСИЛАНЬ

1 А.В. Соколов, В.Ф. Шаньгин Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 656 стр., 2002 г.

2 Постанова Кабінету міністрів України від 9 серпня 2005 р. N 720 "Про затвердження Правил надання та отримання телекомунікаційних послуг".

3 Закон України “Про інформацію”.

4 НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»

5 Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.Фратто М. Механизмы защиты корпоративных сетей //Сети и системы связи. –2002. –№ 2(80). –С. 78-82.

6 Березин А., Перчиков В. Концепция защиты корпоративной сети //Корпоративные системы. –2001. –№4. –С. 65-69.

7 Норткатт С. и др. Анализ типовых нарушений безопасности в сетях. — Киев: Издательство "Вильямс". — 2002.

8 Анализ безопасности управление доступом и информационными потоками в компьютерных системах — М.: Издательство "Радио и связь". — 2004.

9 Мельников В. В. Защита информации в компьютерных системах. — М.: Финансы и статистика; Электроинформ. — 1997.

10 Кримінальний кодекс України.

11 НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

12 Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн.1. - М.:Энергоатомиздат, 1994.

13 А. Ю. Щеглов Защита компьютерной информации от несанкционированного доступа, Наука и Техника, 384 стр., 2004 г.

14 Краткий обзор Microsoft Forefront Online Security for Exchange. Спосіб доступу URL: http://blogs.technet.com/b/kabans/archive/2009/11/25/microsoft-forefront-protection-2010-exchange-server.aspx – Загол. з екрану.

15 Безопасность системы электронной почты. Спосіб доступу URL: http://citforum.ru/security/internet/email/article1.6.2003104.html – Загол. з екрану.

16 Организация комплексной защиты информации. Спосіб доступу URL: http://lib.rus.ec/b/336212/read#t11 – Загол. з екрану.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	22	
6	А4	2 Розділ	24	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка засобів захисту інформаційно-комунікаційної системи підприємства «Фотон» від зловмисної масової розсилки повідомлень
Калістого Дмитра Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Об'єкт дослідження: система захисту корпоративних інформаційних мереж від загроз пов'язаних із зловмисною масовою розсилкою повідомлень.

Мета роботи: розробка методології захисту корпоративних інформаційних систем від загроз пов'язаних із зловмисною масовою розсилкою повідомлень.

У спеціальній частині виконано аналіз загроз інформаційної безпеки корпоративних інформаційних систем, які пов'язані із зловмисною масовою розсилкою повідомлень, проаналізовані методи протидії цим загрозам та розроблена методологія захисту від даного типу загроз.

В економічному розділі проведено розрахунок капітальних та експлуатаційних витрат на проектування та впровадження нового комплексу для захисту від спаму та розраховано економічний ефект від впровадження даного комплексу.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник